Technical and Organizational Measures
Miradore

Executive Summary

This Technical and Organizational Measures ("TOMs") document sets out GoTo's privacy, security and accountability commitments for Miradore. Specifically, GoTo maintains robust global privacy and security programs and organizational, administrative and technical safeguards designed to: (i) ensure the confidentiality, integrity and availability of Customer Content; (ii) protect against threats and hazards to the security of Customer Content; (iii) protect against any loss, misuse, unauthorized access, disclosure, alteration and destruction of Customer Content; and (iv) maintain compliance with applicable law and regulations, including data protection and privacy laws. Such measures include:

- **Encryption**:
  - *In Transit* Transport Layer Security (TLS) v1.2.
  - *At Rest* Azure encryption at host, CMK (Customer managed key) RSA 4096 and Advanced Encryption Standard (AES) 256-bit for Customer Content. Databases are encrypted with AES256.
- **Data Centers:** The data center in Germany supports redundancy and stability.
- **Physical Security:** Suitable physical security and environmental controls are in place and designed to protect, control and restrict physical access for systems and servers that maintain Customer Content to support uptime, performance and scalability commitments.
- **Compliance Audits**: Miradore holds PCI DSS, ISO 27001 and APEC CBPR and PRP certifications.
- **Legal/Regulatory Compliance:** GoTo maintains a comprehensive data protection program with processes and policies, designed to ensure Customer Content is handled in accordance with applicable privacy laws, including the GDPR, CCPA/CPRA and LGPD.
- **Security Assessments**: In addition to in-house testing, GoTo contracts with external firms to conduct regular security assessments and/or penetration testing.
- **Logical Access Controls:** Logical access controls are implemented and designed to prevent or mitigate the threat of unauthorized application access and data loss in corporate and production environments.
- **Data Segregation**: Customer-based database schemas support data segregation and security permissions are applied to separate and protect database objects.
- **Perimeter Defense and Intrusion Detection**: Perimeter protection tools, techniques and services are designed to prevent unauthorized network traffic from entering the product infrastructure. The GoTo network features external-facing firewalls and internal network segmentation.
- **Retention**:
  - Miradore Customers may request the return or deletion of Customer Content at any time which will be fulfilled within thirty (30) days of Customer's request.
  - Customer Content will automatically be deleted ninety (90) days after the end of Customer's then-final subscription term when they cancel or terminate their account.

Table of Contents

Click the page numbers below to go to the relevant TOMs section

1 Product Introduction

Miradore is GoTo's cloud-based mobile device management (MDM) solution for Android and iOS mobile devices and macOS and Windows workstations (the "Service"). Miradore's feature set allows administrators to manage device security, settings and restrictions, data security, app settings, content, automation and reporting—all from a single portal.

Capitalized terms in this document that are not defined within the text are defined in the Terms of Service.

2 Technical Measures

GoTo's products are designed to provide solutions that are secure, reliable and private. The technical measures defined below describe how GoTo implements that design and applies it in practice for Miradore.

2.1 Safeguards

GoTo's implementation of safeguards, features and practices involves:

I. Building security and data protection into products and processes by design and default, including additional layers of security to protect Customer Content;

II. Maintaining organizational controls that operationalize internal policies and procedures related to standards compliance, incident management, application security, personnel security and regular training programs; and

III. Ensuring privacy practices are in place to govern data handling and management in accordance with applicable law, including the GDPR, CCPA/CPRA, LGPD and our own Data Processing Addendum (DPA), as well as applicable GoTo policies and commitments.

By building security safeguards into the product, we strive to protect GoTo Customer Content from threats and ensure security controls are appropriate to the nature and scope of the Service. GoTo's configurable security features can help administrators minimize threats and risks to systems and networks posed by individuals who use GoTo services.

3 Product Architecture

Miradore is a device management solution for mobile devices and workstations featuring a multi-tier architecture. Miradore leverages Microsoft Azure cloud resources to provide a scalable, highly available solution with no single point of failure. Security measures provide in-depth defense at all levels, from the physical layer through the application layer.

There are multiple Miradore interfaces including the main user interface, the web service API, connectors to third-party systems and managed devices.

3.1 The Main User Interface

Miradore's main user interface is the management console. It is browser-based and employs the secure HTTPS protocol between the Service and the managed device.

3.2 Web Service API

The Miradore API is a Representational State Transfer (REST)-based web service that enables Miradore to integrate with external information systems. The API is used over HTTPS with the GET method to export data directly from Miradore's database in XML or JSON format. All API requests are authenticated with authentication keys that are administered in the management console of each Miradore instance. See the API Support Article for more information.

3.3 Miradore in Managed Devices

Devices communicate with the Service's server either through the Miradore client, which is a custom program installed on a workstation or device, or through the platform's integrated mobile device management framework provided by Apple (iOS), Google (Android) or Microsoft (Windows).

To become a managed device in Miradore, a device must go through an enrollment process. The device enrollment process is initiated either by the individual using the device ("End User") or the administrator of a Miradore instance ("User") and is authenticated with one-time enrollment credentials created for each enrollment. If the User initiates the enrollment process, the enrollment credentials are included in the enrollment invitation message sent to the End User by email or SMS. If the End User initiates the enrollment process (self-service), they will use a specific company passcode to enroll the device through the enrollment portal (https://login.online.miradore.com/enroll). To access self-service enrollment, an individual must be listed in in the specific Miradore instance as a device End User. After a successful enrollment, the End User who completed the enrollment will become the assigned End User of that device in Miradore.

Data moves between a managed device and the Service when the Miradore client polls the Service for commands, the Service returns the commands, and the Miradore client posts back the task results. Examples of commands include enforcement of configuration policy settings, software installations and scheduled task results (e.g., hardware and software inventories). If an instant synchronization is needed, the Service can request that a managed device poll the Service immediately through an applicable push notification service.

The vendor push notification services (Apple Push Notification Service, Firebase Cloud Messaging, Azure SignalR and Windows Push Notification Service) are connected to the managed devices and the Service with HTTPS and vendor-specific protocols. Additionally, the Miradore client for macOS, iOS, Windows, and Android platforms is cryptographically signed to authenticate connections with the Service.

Regardless of the device operating system, End Users are always able to see whether their device is managed with Miradore. Typically there is a client application or MDM profile visible to the End Users.

4 Technical Security Controls

GoTo employs technical security controls that are designed to safeguard the Service infrastructure and data residing therein.

4.1 Encryption

GoTo periodically reviews our encryption standards and may update the ciphers and/or technologies used in accordance with the assessed risk and market acceptance of new standards.

4.1.1 Encryption In-Transit

Miradore utilizes HTTPS TLS 1.2 protocols to secure network traffic. All communications in-transit between the End User and the user interface are encrypted.

4.1.2 Encryption At-Rest

All servers are encrypted. At-rest, virtual machine server data is stored with Azure encryption at host and CMK Rivest–Shamir–Adleman (RSA) 4096. Databases are encrypted with service-managed transparent data encryption using encryption algorithm AES 256-bit.

4.2 User Authentication

Users are authenticated with a username and a password which must be at least eight characters long. User passwords are salted and stored in the database as Secure Hash Algorithm (SHA)-512 hashes and are cryptographically signed. All User connections to the Service and actions within the Service are logged and displayed in the action log to provide an audit trail. If a User forgets their password, they can reset it through a Microsoft school or work account or using the password recovery workflow that is built-in to the Service and available through the login screen. The password recovery workflow sends an email to the User containing a hyperlink for resetting the User's password. Two-factor authentication is available for the Service and can be configured by an individual User for their own login or as a requirement set by an administrator for an entire Miradore account.

5 Security Program Updates

GoTo reviews and updates our security program and engages independent third parties to assess our relevant security controls at least annually to ensure we evolve against the current threat landscape and to ensure compliance with relevant frameworks, industry standards, Customer commitments, and, as applicable, changes in laws and regulations pertaining to the security of GoTo data.

6 Data Backup, Disaster Recovery and Availability

GoTo's architecture is designed to perform replication in near real time to geographically diverse locations. Databases are backed up using a rolling incremental backup strategy. In the event of

a disaster or total site failure, the remaining locations are designed to balance the application load. Disaster recovery related to these systems is tested periodically.

Customer Content backup is done within the same data center in 24-hour and seven-day intervals. In addition, a corresponding backup is made in a geographically distant data center every seven days and is retained for four weeks.

Database servers and front-end web servers hosting the Service are backed up daily. Databases have point-in-time restore available for up to 14 days and weekly long-term database backups available for one year. Web servers have instant recovery possible for two days.

Firewalls are used on network connections between the internet and the data center network to only allow connections over HTTPS (port 443) to designated web servers. A load balancer is used to distribute requests evenly among the web servers.

Server hardware, operating systems, and the Miradore Service are continuously being monitored and persons responsible for servers will be alerted in case of deviations in the Service operability.

7 Data Centers

The GoTo infrastructure is designed to increase service reliability and reduce the risk of downtime. The Service is hosted in Microsoft Azure in Germany which includes monitoring of environmental conditions and around-the-clock physical security measures addressed below.

7.1 Data Center Physical security

GoTo contracts with data centers to provide physical security and environmental controls for server rooms that house production servers. These controls include:

- Video surveillance and recording;
- Multi-factor authentication to highly sensitive areas;
- Heating, ventilation and air conditioning temperature control;
- Fire suppression and smoke detectors;
- Uninterruptible power supply;
- Raised floors or comprehensive cable management;
- Continuous monitoring and alerting;
- Protections against common natural and man-made disasters, as required by the geography and location of the relevant data center; and
- Scheduled maintenance and validation of all critical security and environmental controls.

GoTo limits physical access to production data centers to authorized individuals only. Access to an on-premise server room or third-party hosting facility requires the submission of a request through the relevant ticketing system and approval by the appropriate manager, as well as review and approval by GoTo's technical operations team. All physical access to data centers and server rooms is logged and GoTo management reviews logs on at least a quarterly basis. Additionally, data center physical access authorization is removed promptly upon role change (where such access is no longer required) or upon termination of any previously authorized

personnel. Multi-factor access (e.g., biometrics, badge and keypad) is required for highly sensitive areas, which include data centers.

8 Standards Compliance

GoTo regularly assesses our compliance with applicable legal, security. financial, data privacy and regulatory requirements. GoTo's privacy and security programs have met rigorous and internationally recognized standards, been assessed in accordance with comprehensive external audit standards and achieved key certifications, including:

- **TRUSTe Enterprise Privacy & Data Governance Practices Certification** to address operational privacy and data protection controls that are aligned with key privacy laws and recognized privacy frameworks. To learn more, visit our blog post.
- **TRUSTe APEC CBPR and PRP Certifications** for the transfer of Customer Content between APEC-member countries obtained and independently validated through TrustArc, an APEC-approved third-party leader in data protection compliance. To learn more about our APEC certifications, click here.
- International Organization for Standardization – **ISO/IEC 27001:2013** Information Security Management System (ISMS) Certification.
- **Payment Card Industry Data Security Standard (PCI DSS)** compliance for GoTo's eCommerce and payment environments.

9 Application Security

Miradore's application security program follows secure system engineering principles to secure product code during the development lifecycle. At its core, the program employs a security first approach, simple design, defense in depth, least privilege access, input validation, password management, error handling and logging, manual code reviews, and threat modeling. Miradore also uses quality assurance techniques, such as peer code reviews, security testing, penetration testing, and security audits, to ensure the quality and security of the developed information system.

10 Logging, Monitoring and Alerting

GoTo maintains policies and procedures around logging, monitoring and alerting, which set out the principles and controls that are implemented to bolster our ability to detect suspicious activity and respond to them on a timely basis. GoTo collects identified anomalous or suspicious traffic in relevant security logs in applicable production systems.

11 Endpoint Detection and Response

Endpoint Detection and Response software with audit logging is deployed on all GoTo servers to minimize disruption or impact on the performance of the Service. Security investigations will be initiated in accordance with our incident response procedures if suspicious activity is detected, as

appropriate and necessary. See section 17 for more information on GoTo's Security Operations Center and incident response procedures.

12 Threat Management

GoTo's Cyber Security Incident Response Team ("CSIRT") is comprised of multiple teams and is responsible for cyber threat protection. Specifically, the Cyber Threat Intelligence team within the CSIRT collects, vets and disseminates information as it pertains to current and emerging threats. GoTo stays current with threat intelligence and mitigation through review of open and closed sources and participation in sharing groups and industry memberships (IT-ISAC, FIRST.org, etc.).

13 Security and Vulnerability Scanning and Patch Management

GoTo maintains a formal patch management program and, on at least a quarterly basis, performs patch management activities on all relevant systems, devices, firmware, operating systems, applications and other software that process Customer Content. GoTo assesses and scans for system-level, internal and external host/network ("Systems") vulnerabilities, on no less than a monthly basis, as well as after any material change to such Systems and remediates relevant discovered vulnerabilities in accordance with documented policies that prioritize remediation based on risk.

14 Logical Access Control

Logical access control procedures are in place to reduce the risk of unauthorized application access and data loss in corporate and production environments. Employees are granted access to specified GoTo systems, applications, networks and devices based on the principle of least privilege. User privileges are segregated based on functional role (role-based access control) and environment using segregation of duties controls, processes and/or procedures.

15 Data Segregation

GoTo has implemented controls to prevent Users from seeing the data of other Users. Miradore leverages customer-based database schemas and applies security permissions for separating and protecting database objects based on a User's or Customer's GoTo account. Parties must be authenticated to gain access to an account.

16 Perimeter Defense and Intrusion Detection

GoTo uses perimeter protection tools, techniques and services to protect against unauthorized network traffic entering GoTo's product infrastructure. These include, but are not limited to:

- Intrusion detection systems that monitor systems, services, networks, and applications for unauthorized access;

- Critical system and configuration file monitoring to prevent or reduce the likelihood of unauthorized modification;
- Application-layer DDoS prevention service through which GoTo traffic is proxied to block malicious server traffic; and
- Host-based firewalls on GoTo web servers that filter inbound and outbound connections, including internal connections between GoTo systems.

17 Security Operations and Incident Management

GoTo's Security Operations Center is responsible for detecting and responding to security events. The Security Operations Center uses security sensors and analysis systems to identify potential issues and has developed incident response procedures, including a documented Incident Response Plan.

GoTo's Incident Response Plan is aligned with GoTo's critical communication processes, policies and standard operating procedures. It is designed to manage, identify and resolve relevant suspected or identified security events across its systems and services, including GoTo Resolve. The Incident Response Plan sets out mechanisms for employees to report suspected security events and escalation paths to follow when appropriate. Suspected events are documented and escalated as appropriate via standardized event tickets and triaged based upon criticality.

18 Return and Deletion of Customer Content

Deletion and/or Return: Customers may request return and/or deletion of their Customer Content by submitting a request using GoTo's Individual Rights Management Portal ("IRM"), via support.goto.com, or by e-mailing privacy@goto.com. Requests shall be processed within thirty (30) days of receipt by GoTo, or in the unlikely event more time is needed, we will provide notice as soon as possible of any anticipated delayed and revised completion deadline.

Customer Content Retention Schedule: Unless otherwise required by applicable law, Customer Content shall be automatically deleted ninety (90) days after the termination or cancellation and, in each case, deprovisioning of Customer's then-final subscription. If Customer's subscription expires, the account will convert to a free account and may be deleted only if the account has no active Users and no managed devices. Upon written request, GoTo may provide written confirmation/certification of Content deletion.

19 Organizational Controls

19.1 Security Policies and Procedures

GoTo maintains a comprehensive set of security policies and procedures that are periodically reviewed and updated as necessary to support GoTo's security objectives, changes in applicable law, industry standards and compliance efforts.

19.2 Change Management

GoTo maintains a suitable change management process and changes to GoTo Systems are assessed, tested and approved before implementation to reduce the risk of disruption to GoTo services.

19.3 Security Awareness and Training Programs

GoTo's privacy and security awareness program involves training employees about the importance of handling Personal Data and confidential information ethically, responsibly, in compliance with applicable law, and with due care. Newly hired employees, contractors and interns are informed of security policies and the GoTo Code of Conduct and Business Ethics during onboarding. GoTo Employees complete privacy and security awareness training at least annually. Awareness activities take place throughout the year and can include campaigns for Data Privacy Day, Cybersecurity Awareness Month, webinars with the Chief Information Security Officer and a security champions program.

Where appropriate, employees may also be required to complete role-specific trainings. Additionally, all GoTo employees, contractors and subsidiaries must review and adhere to GoTo's policies related to security and data protection.

20 Privacy Practices

GoTo takes the privacy of our Customers, Users and End Users very seriously and is committed to disclosing relevant data handling and management practices in an open and transparent manner.

20.1 Privacy Program

GoTo maintains a comprehensive privacy program that involves coordination from multiple functions within the company, including Privacy, Security, Governance, Risk and Compliance (GRC), Legal, Product, Engineering and Marketing. This privacy program is centered around compliance efforts and involves the implementation and maintenance of internal and external policies, standards and addenda to govern the company's practices.

20.2 Regulatory Compliance

20.2.1 GDPR

The General Data Protection Regulation (GDPR) is a European Union (EU) law regarding data protection and privacy for individuals within the EU. GoTo maintains a comprehensive GDPR compliance program and to the extent GoTo engages in processing of Personal Data subject to the GDPR on behalf of the Customer, we will do so in accordance with the applicable requirements of the GDPR. For more information, visit https://www.goto.com/company/trust/privacy.

20.2.2 CCPA

The California Consumer Privacy Act, as amended by the California Privacy Rights Act (collectively referred to as "CCPA") grants Californians additional rights and protections

regarding how businesses may use their personal information. GoTo maintains a comprehensive compliance program and to the extent GoTo engages in processing of Personal Data subject to the CCPA on behalf of the Customer, we will do so in accordance with the applicable requirements of the CCPA. For more information about our compliance with the CCPA, see GoTo's Privacy Policy and Supplemental California Consumer Privacy Act Disclosures.

20.2.3 LGPD

The Brazilian Data Protection Law (LGPD) regulates the processing of Personal Data in Brazil and/or of individuals located in Brazil at the time of collection. GoTo maintains a comprehensive compliance program and to the extent GoTo engages in processing of Personal Data subject to the LGPD on behalf of the Customer, we will do so in accordance with the applicable requirements of the LGPD. For more information, visit https://www.goto.com/company/trust/privacy.

20.3 Data Processing Addendum

GoTo offers a global Data Processing Addendum (DPA), available in English and German. This DPA meets the requirements for GDPR, CCPA, LGPD and other applicable regulations and governs GoTo's processing of Customer Content.

Specifically, our DPA incorporates several GDPR-focused data privacy protections, including:

(a) data processing details and sub-processor disclosures as required under Article 28;
(b) revised (2021) Standard Contractual Clauses (a.k.a. the EU Model Clauses); and
(c) GoTo's product-specific technical and organizational measures.

Additionally, to account for CCPA requirements, our global DPA includes:

a) revised definitions mapped to the CCPA;
b) access and deletion rights; and
c) warranties that GoTo will not sell our Customer's, Users' and End Users' personal information.

Our global DPA also includes provisions to:

(a) address GoTo's compliance with the LGPD;
(b) support lawful transfers of Personal Data to/from Brazil; and
(c) ensure that our Users enjoy the same privacy benefits as our other global Users.

20.4 Transfer Frameworks

GoTo has a robust global data protection program which takes into account applicable law and supports lawful international transfers under the following frameworks:

20.4.1 Standard Contractual Clauses

The Standard Contractual Clauses (SCCs), sometimes referred to as EU Model Clauses, are standardized contractual terms, recognized and adopted by the European Commission, to ensure that any Personal Data leaving the European Economic Area (EEA) will be transferred in compliance with EU data protection law. The SCCs, revised and issued in 2021, are

incorporated in GoTo's global DPA to enable GoTo Customers to transfer data out of the EEA in compliance with the GDPR.

20.4.2 APEC CBPR and PRP Certifications

GoTo has obtained Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) certifications. The APEC CBPR and PRP frameworks are the first data regulation frameworks approved for the transfer of Personal Data between APEC-member countries and were obtained and independently validated through TrustArc, an APEC-approved third-party data protection compliance vendor.

20.5 Supplemental Measures

In addition to the measures specified in these TOMs, GoTo has created an FAQ designed to outline the supplemental measures implemented to support lawful transfers under Chapter 5 of the GDPR and address and guide any case-by-case analyses recommended by the European Court of Justice in conjunction with use of the SCCs.

20.6 Data Requests

GoTo maintains comprehensive processes to facilitate receiving data protection and security-related requests, including the IRM portal, Privacy email address (privacy@goto.com) and Customer support at https://support.goto.com.

20.7 Sub-Processor and Data Center Disclosures

GoTo publishes Sub-Processor Disclosures on its Trust & Privacy Center (https://www.goto.com/company/trust/resource-center). These disclosures show the names, locations and processing purposes of data hosting providers and other third parties that process Customer Content as a part of providing the Service to GoTo Customers.

20.8 Sensitive Data Processing Restrictions

Unless expressly requested by GoTo or Customer has otherwise received written permission from GoTo, the following types of sensitive data must not be uploaded or otherwise provided to GoTo:

- Government-issued identification numbers and images of identification documents.
- Information related to an individual's health, including, but not limited to, Personal Health Information (PHI) as identified in the U.S. Health Insurance Portability and Accountability Act (HIPAA), as well as other relevant applicable laws and regulations.
- Information related to financial accounts and payment instruments, including, but not limited to, credit card data. The only general exception to this provision extends to explicitly identified payment forms and pages that are used by GoTo to collect payment for the Service.
- Any information especially protected by applicable laws and regulation, specifically information about individual's race, ethnicity, religious or political beliefs, organizational memberships, etc.

20.9 Compliance in Regulated Environments

Customers are responsible for implementing appropriate policies, procedures and other safeguards related to their use of GoTo Resolve to support devices in regulated environments.

21 Security and Privacy Third-Party Controls

Prior to engaging third-party vendors that process Customer Content or confidential, sensitive, or employee data, GoTo reviews and analyzes the vendor's security and privacy practices using the appropriate Procurement channels. As appropriate, GoTo may obtain and evaluate compliance documentation or reports from vendors periodically to ensure their control environment and standards continue to be sufficient.

GoTo enters into written agreements with all third-party vendors and either utilizes GoTo-approved procurement templates or negotiates such third parties' standard terms and conditions to meet GoTo-accepted privacy and security standards, where deemed necessary. The Finance, Legal, Privacy and Security teams are involved in the vendor review process and verify that vendors meet specific mandatory data handling and contractual requirements, as necessary and/or appropriate. GoTo's third party risk policies govern privacy and security requirements of vendors on the basis of type and duration of data processing and level of access. Where appropriate (e.g., where Customer Content is processed or stored), agreements with vendors include "compliance with applicable law" requirements, a DPA or similar document that addresses topics such as GDPR, CCPA, LGPD and use and sale restrictions, as appropriate. For instance, GoTo's Supplier DPA has restrictions around data "selling" as defined under the CCPA. Similarly, security addenda with suitable controls and systems requirements are put in place with relevant vendors.

22 Contacting GoTo

Customers can contact GoTo at support.goto.com for general inquiries. For questions or requests related to Personal Data or privacy, please visit our IRM portal or send an email to privacy@goto.com.